International A Levels Information Technology

Unit 1 Notes

1.3 Unit content

Topicwise Question papers, Mark schemes and Examiners' Reports

Topic 1: Hardware and software

Digital devices consist of both hardware and software components. From the hardware perspective, it is important to understand the technologies that enable these devices. From the software perspective, it is important to understand licensing and maintenance. Understanding both the hardware and software will enable students to assess and select components to meet the requirements of an individual, organisation or scenario.

What students need to learn

1.1 Hardware

1.1.1 Understand the features and functions of contemporary digital devices.

Portability

- Portability is a key feature of many contemporary digital devices, especially mobile phones and tablets. These devices are designed to be carried around and used on the go.
- Wearable computers, such as smartwatches, are becoming increasingly popular as they allow users to access information and control devices without needing to take out their mobile phone.
- Microprocessors/single board computers are often used for embedded

systems, such as in cars or appliances, where compact size is important.

Performance

- High performance is important for devices that need to process large amounts of data quickly, such as computers and supercomputers.
- Games consoles are also designed for high performance, with powerful processors and graphics cards to handle demanding games.
- Microprocessors/single board computers are often used for specific tasks that require high processing power, such as in robotics or data processing.

Storage

- All contemporary digital devices have some form of storage, such as hard drives, solid-state drives, or removable storage media.
- Network-attached storage (NAS) is a type of storage that can be accessed by multiple devices over a network. This allows for easy sharing of files and resources.
- RAID storage is a type of storage that uses multiple hard drives to protect against data loss in case of a drive failure.

User interface

- The user interface of a digital device refers to how the user interacts with the device. This includes input devices, such as keyboards and touch screens, and output devices, such as monitors and speakers.
- The design of the user interface is an important consideration for manufacturers, as it can affect the usability of the device.
- Some devices, such as biometric scanners and barcode readers, provide additional input methods for secure authentication or data input.

Connectivity

- Connectivity is important for allowing devices to share data and resources. This can be done through cables, such as USB and HDMI, or wirelessly using Wi-Fi, Bluetooth, or other wireless standards.
- Devices such as printers and scanners often have multiple connectivity options to make it easier for users to connect to them.
- Some devices, such as microprocessors/single board computers (Raspberry Pi, Arduino), can be connected to sensors and other devices to allow for data

collection and processing.

Media support

- Contemporary digital devices support a wide range of media formats, including audio, video, and images.
- Some devices, such as cameras and scanners, are specifically designed for capturing media.
- Other devices, such as smart TVs and games consoles, are designed to display high-quality video and graphics.

Energy consumption

- Energy consumption is an important point to consider for manufacturers, as it affects the cost of running the device and its impact on the environment.
- Mobile phones and tablets often have batteries that can be recharged, while other devices are designed to be always plugged in.
- Some devices, such as smart thermostats, are designed to be energy-efficient to reduce their impact on the environment.

Expansion capability

- Some devices, such as computers and microprocessors/single board computers, have expansion slots for adding additional hardware, such as graphics cards or network cards.
- Network-attached storage (NAS) can be expanded by adding additional hard drives to increase storage capacity.
- Other devices, such as printers and scanners, can be expanded by adding additional trays or modules to allow for more functionality.

Security features

- Security is an important consideration for many digital devices, especially those that store sensitive information or are used for secure transactions.
- Devices such as biometric scanners and chip and pin devices provide secure authentication to prevent unauthorised access.
- RAID storage provides redundancy and protects against data loss in case of a drive failure.

Primary Storage:

RAM (Random Access Memory)

- Fast, quickly accessible
- volatile (loses data when power turned off)
- Usually low storage capacity compared to secondary storage.

ROM (Read Only Memory):

- Fast
- Can be read from but not written to
- Holds BIOS/firmware which is needed to load the Operating System (OS)

Types:

- PROM (Programmable ROM)
- EPROM (Erasable Programmable ROM)
- EEPROM (Electrically Erasable Programmable ROM)

Cache:

- L1, L2, and L3 caches inside processor
- Very fast memory
- Very expensive
- L1 is fastest, L3 is slowest
- Store most frequently accessed data

Processors:

- x86 Architecture most common (Intel and AMD processors)
    - High performance
    - Upgradeable parts
    - Relatively old
    - Used in desktops and laptops

- ARM architecture is SoC (System on Chip) (Snapdragon, Apple M1)
    - Relatively lower performance
    - More efficient
    - Everything in one chip
    - Newer
    - Not upgradeable

- Performance
    - More cores
    - Faster clock speed
    - More cache

Storage Devices

Magnetic Tape:

- Magnetised bits of tape
- Very high capacity

- Very cheap
- Very slow read/write speeds

Optical Hard Drives:
- Moving disks have magnetised bits that are read/written by a head
- High storage capacity (1-32 TB)
- Inexpensive
- Slow read/write speeds
- May be damaged by shock
- Large magnet can erase all data on it

Solid State Drives:
- Very fast read/write speeds
- Expensive
- No moving parts so resistant to damage
- Low power
- Relatively low storage capacity

Removable Solid State (SSID) Cards - SD Cards:
- Mid price range
- Very small and portable
- Used in phones and cameras as expandable storage
- Low power, medium capacity

Network Attached Storage (NAS):
- Normal storage devices connected to a network
- Remotely accessible
- Susceptible to network failure

RAID Storage:
- Replicate data over multiple drives
- Increases data reliability and I/O performance

Cables

- HDMI (High Definition Multimedia Interface): capable of transmitting audio and video signals at high speeds of up to 18 Gbps, making it ideal for high-definition multimedia content such as 4K and 8K video.

- USB (Universal Serial Bus): a versatile interface that can transfer data at speeds of up to 10 Gbps (USB 3.2 Gen 2x2), with backwards compatibility to older USB versions.

- Ethernet: a wired network technology that can transmit data at speeds of up to 10 Gbps (10GBASE-T), with faster speeds of up to 40 Gbps and 100 Gbps available for enterprise-level networking.

- DisplayPort: a video interface that can transmit audio and video signals at

high speeds of up to 32.4 Gbps (DisplayPort 2.0), making it ideal for high-resolution displays and gaming.

- Thunderbolt: a high-speed interface developed by Intel that can transfer data at speeds of up to 40 Gbps (Thunderbolt 3), with support for multiple protocols such as USB, DisplayPort, and PCIe.

Note that the speeds listed above are theoretical maximums and actual data transfer rates may be lower depending on various factors such as **cable length, device compatibility, and signal interference**.

1.1.2 Understand the technologies used by digital devices and how they impact on the design and uses of devices:

Global Positioning System (GPS)

allows devices to determine their location and track movements, enabling applications such as navigation, location-based services, and geotagging.

Biometrics

enables devices to recognise and authenticate users based on physical characteristics such as fingerprints, iris, face or voice, improving security and convenience for access control and payment systems.

Touchscreen

allows users to interact with devices through touch, simplifying user interface design and enabling new forms of interaction such as pinch-to-zoom and swipe gestures.

Sensor

provides devices with the ability to detect and respond to changes in their environment, such as movement, light, temperature, and pressure, enabling features such as automatic screen rotation, ambient light adjustment, and fitness tracking.

Memory

enables devices to store and retrieve data quickly and efficiently, improving performance and enabling features such as multitasking and fast app switching.

Storage

provides devices with the ability to store large amounts of data, such as documents, music, and videos, enabling users to access their content on-the-go.

Battery power

provides devices with the ability to operate untethered from a power source, enabling mobility and convenience, while advances in battery technology have led to longer battery life and faster charging times.

Miniaturisation

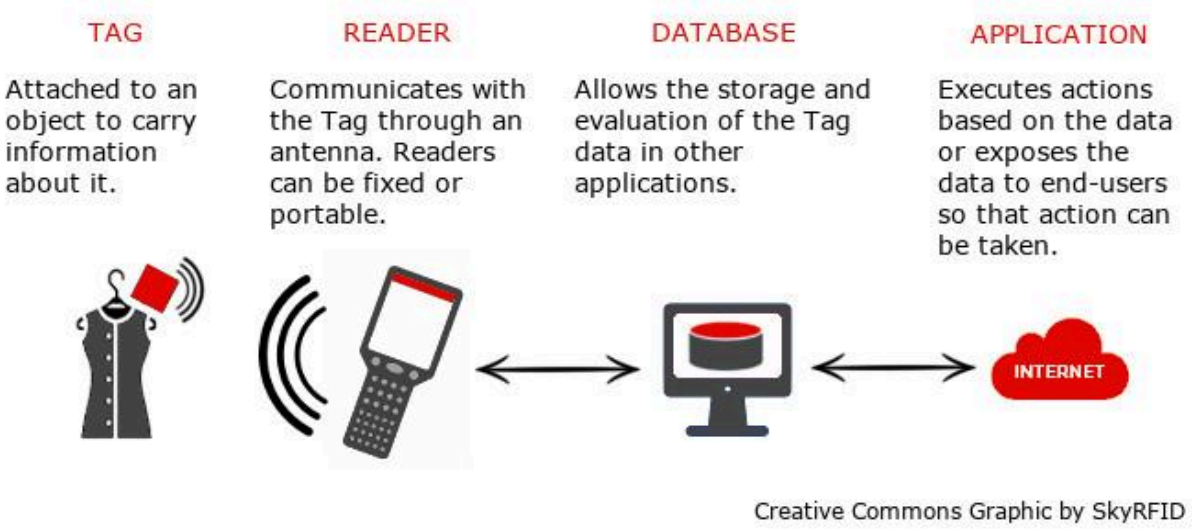
enables devices to become smaller and more portable, while maintaining or improving their performance and functionality.

Processor

provides devices with the computing power to perform complex tasks, such as running applications, processing images, and playing games, while advances in processor technology have led to faster performance and improved energy efficiency.

Radio-frequency identification (RFID)

enables devices to identify and track objects using radio waves, enabling applications such as inventory management, contactless payment, and access control.


TAG
Attached to an object to carry information about it.
READER
Communicates with the Tag through an antenna. Readers can be fixed or portable.
DATABASE
Allows the storage and evaluation of the Tag data in other applications.
APPLICATION
Executes actions based on the data or exposes the data to end-users so that action can be taken.
INTERNET
Creative Commons Graphic by SkyRFID

- RFID stands for radio-frequency identification, and it uses radio waves to automatically identify and track objects.
- An RFID system consists of a reader and a tag. The reader sends out a radio signal that powers up the tag, allowing it to send back its unique identification number.
- RFID tags can be either passive, meaning they don't have a power source and are powered by the reader's signal, or active, meaning they have a

built-in battery and can transmit their signal over longer distances.

- It is used in a variety of applications, such as inventory management, supply chain tracking, and access control.
- RFID tags can be attached to a wide range of objects, including products, vehicles, and even people or animals.
- In retail, RFID can be used to track inventory in real-time, reducing out-of-stock situations and increasing sales.
- In logistics and supply chain management, RFID can help track the movement of goods through the supply chain, improving efficiency and reducing errors.
- In healthcare, RFID can be used to track medical equipment and supplies, monitor patients, and improve patient safety.
- In access control, RFID can be used to grant or restrict access to buildings, rooms, and equipment.

Overall, RFID provides a reliable, efficient, and cost-effective way to track and manage objects, improving business operations and enhancing customer experiences.

Near-field communication (NFC):

enables devices to exchange data wirelessly over short distances, enabling applications such as mobile payments, transit ticketing, and data transfer between devices.

How NFC Works:

- NFC (Near Field Communication) is a wireless communication technology that allows two devices to communicate when they are placed in close proximity to each other.
- NFC uses magnetic field induction to transmit data between devices.
- NFC operates at a frequency of 13.56 MHz and has a range of about 4 centimetres.
- NFC works by modulating a magnetic field to transmit data between two devices. It can transmit encrypted data.

Applications:

- NFC is commonly used for contactless payments, allowing users to make

purchases by tapping their smartphone or other NFC-enabled device against a payment terminal.

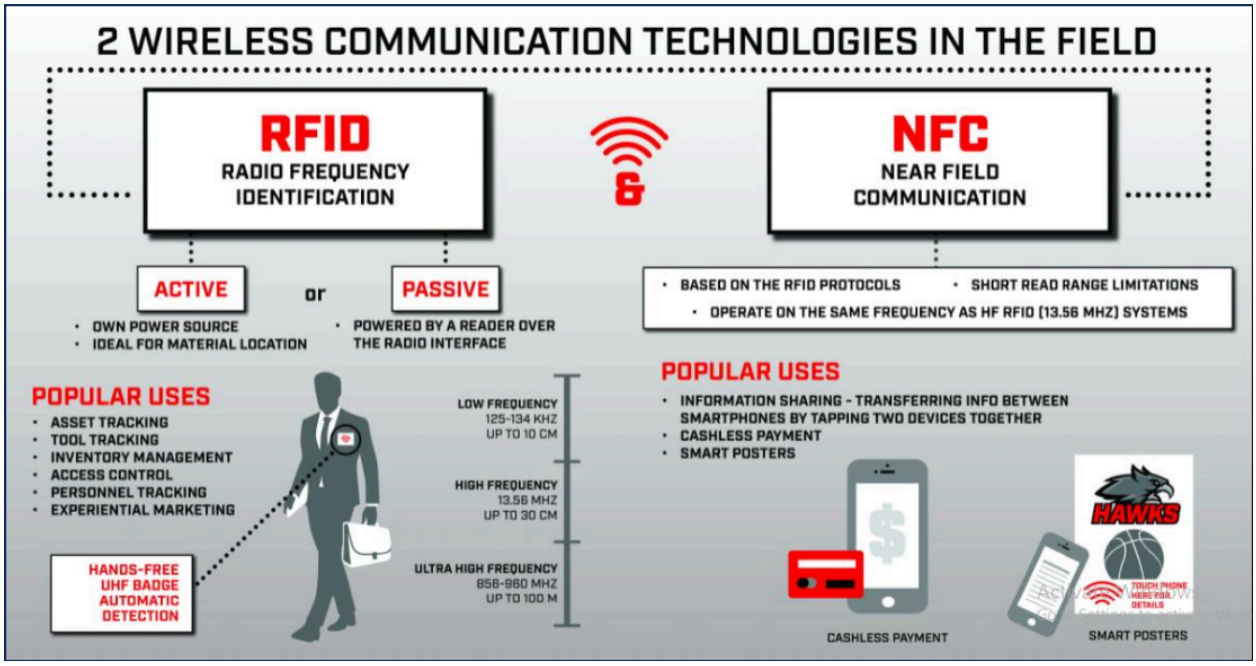
- NFC can also be used for data transfer between two devices. For example, users can transfer photos, videos, and other files between smartphones or other devices using NFC.

- NFC is used in access control systems to allow users to gain entry to a building or secure area by tapping an NFC-enabled card or device against a reader.

- NFC tags can be used to provide information to users, such as directions or product information. Users can tap their smartphone against an NFC tag to access this information.

- NFC can be used in transportation systems to allow users to pay for fares or access information about schedules and routes using an NFC-enabled device.

- NFC can be used in healthcare systems to manage patient information and provide access to medical records using an NFC-enabled device.


2 WIRELESS COMMUNICATION TECHNOLOGIES IN THE FIELD
RFID
RADIO FREQUENCY IDENTIFICATION
&
NFC
NEAR FIELD COMMUNICATION
ACTIVE
or
PASSIVE
• OWN POWER SOURCE
• IDEAL FOR MATERIAL LOCATION
• POWERED BY A READER OVER THE RADIO INTERFACE
• BASED ON THE RFID PROTOCOLS
• SHORT READ RANGE LIMITATIONS
• OPERATE ON THE SAME FREQUENCY AS HF RFID (13.56 MHZ) SYSTEMS
POPULAR USES
• ASSET TRACKING
• TOOL TRACKING
• INVENTORY MANAGEMENT
• ACCESS CONTROL
• PERSONNEL TRACKING
• EXPERIENTIAL MARKETING
HANDS-FREE UHF BADGE AUTOMATIC DETECTION
LOW FREQUENCY 125-134 KHZ UP TO 10 CM
HIGH FREQUENCY 13.56 MHZ UP TO 30 CM
ULTRA HIGH FREQUENCY 856-960 MHZ UP TO 100 M
POPULAR USES
• INFORMATION SHARING - TRANSFERRING INFO BETWEEN SMARTPHONES BY TAPPING TWO DEVICES TOGETHER
• CASHLESS PAYMENT
• SMART POSTERS
HAWKS
CASHLESS PAYMENT
SMART POSTERS

Quick response (QR) code:

enables devices to quickly and easily access information by scanning a code using their camera, enabling applications such as marketing, advertising, and authentication.

How QR Codes Work:

- QR codes (Quick Response codes) are two-dimensional barcodes that can be scanned using a smartphone or other mobile device.
- QR codes are made up of black and white squares arranged in a specific pattern.
- When a QR code is scanned, the device uses its camera to capture the pattern and then decodes the information contained in the code.
- **QR codes can contain various types of information, such as website URLs, contact information, product information, and more.**
- **QR codes have:**
    - **URLs**
    - **Alignment Markers**
    - **Position Markers**
    - **QR Code version**
    - **Date/Time Info**
    -

Applications:

- commonly used in marketing and advertising to provide additional information to consumers. For example, a QR code on a product packaging can be scanned to provide product details, user reviews, or promotional offers.
- ticketing systems, such as for airline or event tickets. Users can scan a QR code to access their ticket information.
- payment systems to allow users to make payments by scanning a code with their smartphone or other device.
- inventory management to track and manage products. QR codes can be printed on product labels or packaging to help identify and track items.
- education to provide students with additional information or resources. For example, a QR code on a textbook can be scanned to access interactive content or study materials.
- used in contact tracing during the COVID-19 pandemic. Users can scan a QR code when entering a public space or event to help track potential exposure

to the virus.

Connectivity:

enables devices to connect to the internet and other devices, enabling features such as messaging, social networking, cloud storage, and remote access. Advances in connectivity technology have led to faster speeds, greater coverage, and improved reliability.

1.1.3 Understand the term 'technological convergence' in the context of digital devices.

When two or more separate technologies/devices merge into one. For example, smartphones can do most things a laptop can and it is more portable.

Another example would be gaming consoles evolving beyond just games and now including streaming services like Netflix and Spotify.

Smart watches not only tell the time but have taken the jobs of health monitoring systems.

1.1.4 Understand the concept of and the need for features and functions of embedded systems.

Embedded systems:

Concept of Embedded Systems:

An embedded system is a computer system designed to perform a specific function within a larger system or product.

It is typically a combination of hardware and software components that work together to accomplish a specific task.

Examples of embedded systems include smart home devices, medical equipment, automotive systems, and industrial machinery.

Need for Features and Functions:

Embedded systems must be designed to meet specific requirements and constraints, such as power consumption, size, and cost.

They often have limited resources, such as memory, processing power, and input/output capabilities.

Therefore, the features and functions of embedded systems must be carefully chosen and optimised to meet the requirements while operating within the resource constraints.

The features and functions of embedded systems can vary widely, depending on the

application, but may include sensing, actuating, processing, communication, and control.

In addition, the reliability and safety of embedded systems are critical, particularly in applications such as medical devices and automotive systems.

Pros:

- Embedded systems are highly specialised and can be optimised for specific tasks, resulting in high performance and efficiency.
- They can operate in real-time, providing fast and accurate responses to external events and inputs.
- Embedded systems are often designed to be low-power, making them suitable for use in battery-powered or energy-efficient devices.
- They can be highly reliable and secure, with built-in safety features and protection against cyber threats.

Cons:

- The highly specialised nature of embedded systems can make them expensive to develop and maintain.
- They can be challenging to debug and troubleshoot, especially in complex systems where multiple components interact with each other.
- The limited resources of embedded systems can result in trade-offs between performance, features, and cost.
- The custom nature of embedded systems can make it difficult to update or upgrade them over time, which can lead to compatibility issues and obsolescence.

1.1.5 Understand the concept of and the need for firmware, including where it is stored.

Concept of Firmware

- Firmware is a type of software that is embedded in hardware devices, such as microcontrollers and system-on-chips (SoC)
- It provides low-level control of the device's hardware components and interfaces with other software components to perform specific tasks

Need for Firmware

- Firmware is critical for the proper functioning of many hardware devices, providing the necessary control and management of the device's components

- It is often responsible for booting up the device and **performing initialization routines**, as well as **managing memory**, **communication interfaces**, and **other hardware components**

- Firmware is also necessary for enabling the device to interact with other software components, such as drivers and operating systems

- In addition, firmware can provide **security features**, such as encryption and authentication, to protect the device from unauthorised access and tampering speed

Where Firmware is Stored

- Firmware is typically stored in non-volatile memory (ROM), which allows it to be retained even when power is turned off.

- The specific location of the firmware can vary depending on the device and its architecture, but it is often stored in on-chip memory, flash memory, or external storage devices, such as EEPROM or SD cards.

- In some cases, firmware can be updated or modified after the device has been manufactured, either through a physical interface or wirelessly via a network connection.

1.1.6 Understand factors that can be used to assess the performance of digital devices:

Speed:

- Refers to the rate at which a device can complete tasks and process data

- Measured in units such as GHz, Mbps, and FPS

- Example: A computer with a higher processor speed can run applications faster than a computer with a lower processor speed.

Capacity:

- Refers to the amount of data that a device can store and process

- Measured in units such as GB, TB

- Example: A hard drive with a larger capacity can store more data than a hard drive with a smaller capacity.

Portability:

- Refers to how easily a device can be transported from one place to another
- Factors that affect portability include weight, size, and durability
- Example: A smartphone is more portable than a desktop computer.

Bandwidth:

- Refers to the amount of data that can be transferred over a network connection in a given amount of time
- Measured in units such as Mbps and Gbps
- Example: A device with a higher bandwidth can download files from the internet faster than a device with a lower bandwidth.

Power efficiency:

- Refers to how efficiently a device uses energy to perform its functions
- Measured in units such as watts and volts
- Example: A laptop with a more power-efficient processor can operate for longer on battery power than a laptop with a less power-efficient processor.

1.1.7 Be able to calculate data file size and time needed to transmit a file.

Same as IGCSE Computer Science

1.2.3 Calculating File Sizes - Revise GCSE Computer Science

Grayscale (black and white):

images uses one byte per pixel (a byte being 8 bits).

- Eight bits means that a byte can store up to 256 levels of information.
- We can therefore store up to 256 levels of brightness per pixel – which gives us what is called '8-bit grayscale'.

Calculating image sizes:

- If we need to calculate the storage requirements of a black and white bitmap image, we multiply the number of pixels wide by the number of pixels high.
- The answer will give us the number of bits.
- We then convert the number into an appropriate unit (kilobytes/megabytes).

Example: 800 by 900 resolution grayscale image size

$800 * 900 = 720,000\ bits$

$720,000 / 8 = 90,000\ bytes$

$90,000 / 1000 = 90\ KB$

Colour depth is the number of bits used to represent each pixel.

- Size in bits = W × H × D
- Size in bytes = W × H × D/8
- W = image width, H = image height, D = colour depth in bits.

Sound

Sampling

- Bit depth defines the dynamic range of the sound – the amplitude (volume) of the waveform at each sample point.

- Quantisation is the name of the audio snapshot when it has to be rounded off to the nearest available digital value.

- Sample rates are measured in hertz (Hz) or thousands of hertz (kHz, kilohertz). For example, 44.1 kHz is equal to 44,100 samples of audio recorded every second.

- The sample rate you choose depends on what the audio is going to be used for. If you wanted to record a song to put on a CD you would usually use 44.1 kHz.

Calculation

- We can calculate sound file sizes based on the sample rate and the sample resolution using the following formula: **File size (bits) = rate × res × secs**

- If we want 30 seconds of mono sound, where the sample rate is 44,100 Hz and the sample resolution is 8 bits, we will have:

  $(44100 \times 8 \times 30)/(8 \times 1000)$

[divided by 8 as we have 8 bits in a byte and 1000 to get kB]

= 1323 KfB

= 1.323 MB

• The size of 30 seconds of stereo sound would be:

$(44100 \times 8 \times 2 \times 30)/(8 \times 1000) = 2646\ kB = 2.6\ MB$

Notes by @uzayermasud

1.1.8 Be able to use and convert between binary and denary, as defined by the International Electrotechnical Commission (IEC). (These are different from SI units.)

IEC Binary vs SI Units

Understand the difference between binary and denary units:

- Binary units are based on powers of two (e.g. 2^0, 2^1, 2^2, etc.), and are commonly used in computing and digital electronics.
- Denary units, also known as decimal units, are based on powers of ten (e.g. 10^0, 10^1, 10^2, etc.), and are commonly used in everyday life.

Know the IEC prefixes for binary units:

Kibibyte (KiB) 2^{10} bytes
Mebibyte (MiB) 2^{20} bytes
Gibibyte (GiB) 2^{30} bytes
Tebibyte (TiB) 2^{40} bytes

Understand the difference between IEC and SI prefixes:

- The International System of Units (SI) uses decimal prefixes, such as kilo-, mega-, and giga-.
- The IEC uses binary prefixes, such as kibi-, mebi-, and gibi-.
- **This means that the size of a kibibyte is 1024 bytes, whereas the size of a kilobyte in SI units is 1000 bytes.**

Kilobyte (KB) 10^3 bytes
Megabyte (MB) 10^6 bytes

Gigabyte (GB) 10^9 bytes
Terabyte (TB) 10^{12} bytes

Use conversion factors to convert between binary and denary units:

- To convert from binary to denary units, multiply the binary value by the appropriate power of two (e.g. 2^10 for kilobytes, 2^20 for megabytes, etc.).
- To convert from denary to binary units, divide the denary value by the appropriate power of two and round down to the nearest integer (e.g. divide by 1024 for kilobytes, 1,048,576 for megabytes, etc.).

Be aware of potential confusion and use the correct units:

- In everyday use, kilobytes, megabytes, and gigabytes are often used to refer to both binary and denary units, which can cause confusion.
- To avoid confusion, use the correct units for the context:
    - such as kibibytes, mebibytes, and gibibytes for binary units
    - kilobytes, megabytes, and gigabytes for denary units.

1.1.9 Be able to select digital devices to meet the needs and requirements of individuals and organisations.

Comes up in questions often, usually with no correct answer. They just want you to talk about the pros and cons of things.

1.2 Software

1.2.1 Understand the purpose of:

- Systems software
- Applications software.

Application software:

- Application software is designed for specific tasks or functions, such as word processing, photo editing, or accounting.

- Application software can be purchased or downloaded by users to perform specific tasks or functions.

- Application software is designed to be user-friendly and easy to use, with intuitive interfaces and features that make it easy to perform specific tasks.

- Application software can be customised and configured to meet the specific needs of individual users or organisations.

- Examples of application software include Microsoft Word, Adobe Photoshop, and QuickBooks.

System software:

- System software is designed to manage and control the operation of the computer system.

- System software is essential for the proper functioning of the computer system, and includes operating systems, device drivers, and utility programs.

- Operating systems are the most important type of system software, providing the interface between the hardware and the user, and managing resources such as memory, storage, and processing power.

- Device drivers are used to control hardware devices such as printers, scanners, and cameras, allowing them to be used with the computer system.

- Utility programs are used to perform specific tasks such as file compression, disk cleanup, and virus scanning.

- System software is typically installed by the manufacturer or system administrator and is not typically customised or configured by individual users.

- Examples of system software include Microsoft Windows, MacOS, and Linux.

1.2.2 Understand the role of the operating system in managing:

- devices
- processes
- users
- security

Devices:

- The operating system manages the interaction between the computer hardware and software.

- The operating system communicates with device drivers to control input and output operations for devices such as keyboards, mice, and printers.

- The operating system also manages the connection and configuration of hardware devices such as external hard drives and USB devices.

Processes:

- The operating system is responsible for managing the allocation of system resources to different processes.

- The operating system manages the scheduling of processes and ensures that they have access to the CPU and memory when needed.

- The operating system also monitors and manages the use of system resources to prevent conflicts and ensure the smooth operation of the system.

Users:

- The operating system provides a platform for users to interact with the computer system.

- The operating system manages user accounts and permissions, ensuring that users only have access to the resources they are authorised to use.

- The operating system also provides a graphical user interface (GUI) that allows users to interact with the computer system in a user-friendly way.

Security:

- The operating system provides a range of security features to protect the computer system from unauthorised access and malicious software.

- The operating system manages user authentication and access control, ensuring that only authorised users have access to the system.

- The operating system also provides security features such as firewalls, antivirus software, and encryption to protect the system from external threats.

- The operating system monitors system activity and logs events, allowing administrators to detect and respond to security breaches and other issues.

1.2.3 Understand the different sources of software and copyright types:

- free
- open-source
- proprietary
- creative commons.

Sources of Software:

- **Free Software:** Software that can be used, modified, and distributed freely without any restrictions. Examples include the GNU/Linux operating system and the Apache web server.

- **Open Source Software:** Software that is available for free and provides access to the source code, allowing users to modify and distribute it. Examples include the Firefox web browser and the MySQL database.

- **Proprietary Software:** Software that is owned and licensed by a specific company, and its source code is usually not available. Examples include the Microsoft Windows operating system and the Adobe Photoshop.

- **Creative Commons Software:** A type of software that is released under a Creative Commons licence, which allows others to use, modify, and distribute the software under certain conditions. Examples include the Creative Commons licence for the Scratch programming language.

Copyright Types:

- **Free:**
    - Allows users to access and use copyrighted material without cost.
    - Examples include freeware, public domain, and some Creative Commons licences.
- **Open Source:**
    - Software whose source code is made available to the public for use and modification.
    - Generally requires attribution to original creators.
    - Examples include Linux, Apache, and Mozilla Firefox.
- **Proprietary:**
    - Refers to copyrighted material that is owned by a person or company and is protected by law.
    - Users must obtain permission to use or access the material.

- Examples include Microsoft Office and Adobe Photoshop.

- **Creative Commons:**

    - A set of licences that allows creators to share their work while retaining some rights.

    - Allows creators to choose the level of freedom they want to give to others to use and modify their work.

    - Examples include Attribution (acknowledgement), No Derivatives (no changing), Public Domain (all rights released), Non-Commercial (no selling) licences.

1.2.4 Understand licensing options:

Licensing Options:

Single User Licence:

This licence allows a single user to use the software on a single device or computer.

- Pros: Simple to manage and cost-effective for individuals or small teams.

- Cons: May not be suitable for larger organisations, and may require additional licences for additional devices or users.

Multiple User Licence:

This licence allows multiple users to use the software on multiple devices or computers, typically with a limit on the number of users or devices.

- Pros: Cost-effective for larger organisations, and easier to manage than multiple single-user licences.

- Cons: May not be suitable for very large organisations or those with fluctuating user/device needs.

Institutional Licence:

This licence allows a group or organisation to use the software on multiple devices or computers within the same institution, such as a school or business.

- Pros: Cost-effective for institutions with many users and devices, and may provide centralised management options.

- Cons: May not be suitable for very large or distributed organisations, and may require additional licences for additional institutions.

Fixed Term Licence:

This licence grants the user the right to use the software for a specified period of time, after which the licence expires and the user must renew it to continue using the software.

- Pros: May be cost-effective for short-term projects or temporary use, and allows users to try out the software without committing to a long-term licence.

- Cons: Can be more expensive in the long run for continued use, and may require additional administrative effort for licence renewal.

Indefinite Licence:

This licence grants the user the right to use the software indefinitely, without any time limit or expiration date.

- Pros: Provides maximum flexibility and long-term cost-effectiveness for continued use, and may provide access to software updates and support.

- Cons: Can be more expensive initially, and may require additional administrative effort for licence management and updates.

Network License:

This licence allows multiple users to access the software on a network, typically with a limit on the number of simultaneous users.

- Pros: Cost-effective for larger organisations, and allows users to access the software from multiple devices.

- Cons: May require additional setup and administrative effort for network management, and may limit simultaneous user access.

Note: There may be other types of licences available, such as subscription licences or open source licences, but these are the main types commonly used in commercial software.

1.2.5 Understand the purpose of, and how to manage, software updates:

- patch
- automatic
- upgrade
- compatibility issues.

Purpose:

- Software updates are released to fix bugs, improve performance, and add new features to existing software.
- Updates may also include security fixes to address vulnerabilities that could be exploited by malicious people.
- In some cases, updates may be required to ensure compatibility with other software or hardware.

Managing Software Updates:

- Software updates can be managed manually or automatically.
- **Automatic updates** are typically enabled by default in most operating systems and applications, and will install updates as they become available without any user intervention.
- **Manual updates** can be initiated by the user through the operating system or application settings.
- **Patches** are a type of update that address specific issues or vulnerabilities in the software. They can be installed manually or automatically.
- **Upgrades** are major releases of software that typically include significant new features or functionality. Upgrades may require a separate purchase or subscription.
- **Compatibility issues** can occur when updates are installed on systems or devices that are not compatible with the updated software. It's important to check compatibility requirements before installing updates to avoid potential issues.

Tips for managing software updates:

- Keep your operating system and applications up-to-date to ensure that you have the latest security patches and features.
- Check for compatibility requirements before installing updates to avoid potential issues.
- Back up important data before installing updates, in case something goes wrong during the update process.
- Consider enabling automatic updates to ensure that you are always running the latest version of the software.

- Be cautious when installing updates from unknown sources, as they could potentially contain malware or other security threats.

1.2.6 Be able to select software to meet the needs and requirements of individuals and organisations.

Topic 2: Networks

Computer networks are essential to most organisations, enabling them to access their information irrespective of its geographical location; make efficient use of hardware and software resources, and communicate effectively. Network design, based on an understanding of protocols, is fundamental to the way networks work. Such reliance on networks in our society is founded on the assumption that there are mechanisms for securing access to them.

What students need to learn

2.1 Network models and protocols

2.1.1 Understand the features and functions of computer network models:

Client-server network model

- Features: In a client-server network model, there is a central server that manages and controls the network resources. Clients, or end-user devices, connect to the server to access these resources.
- Functions: The server provides resources and services such as file storage, email, and web hosting, while the clients request and use these resources.
- Examples: Corporate networks, email servers, and web servers.
- Pros: Centralised control, increased security, scalability, and easier management.
- Cons: High cost, single point of failure, and high maintenance requirements.

Peer-to-peer network model

- Features: In a peer-to-peer network model, all devices are equal and can function as both clients and servers. Each device shares its resources and services with other devices on the network.
- Functions: Devices communicate and share resources with each other without a central server.

- Examples: File sharing networks, gaming networks, and social media.
- Pros: Low cost, easy setup, and no single point of failure.
- Cons: Security risks, limited scalability, and potential performance issues.

Ad hoc network model

- Features: In an ad hoc network model, devices connect directly to each other without the need for a central infrastructure. This type of network is often used for temporary or emergency communications.
- Functions: Devices communicate and share resources with each other without the need for a centralised server or infrastructure.
- Examples: Mobile device to mobile device connections, emergency response networks.
- Pros: Easy setup, flexible and adaptable, and can be used in remote areas.
- Cons: Limited range, limited scalability, and potential security risks.

Tethering

- Features: Tethering involves using a mobile device's cellular data connection to provide internet access to other devices. The tethered device acts as a mobile hotspot, allowing other devices to connect to it and use its internet connection.
- Functions: The tethered device shares its internet connection with other devices.
- Examples: Using a smartphone as a hotspot for a laptop or tablet.
- Pros: Easy to set up, widely available, and can be used in areas without Wi-Fi.
- Cons: Limited range, limited bandwidth, and potential data usage restrictions and additional costs from cellular providers.

2.1.2 Understand the features and purposes of network communication protocols:

Wi-Fi

- Provides wireless access to the internet or a network

- Uses radio waves to transmit data between devices
- Allows multiple devices to connect simultaneously
- Use cases: internet browsing, file sharing, streaming media
- Example devices: smartphones, laptops, tablets, smart TVs, gaming consoles, home assistants

ZigBee

- Designed for low-power, low-data-rate wireless communication
- Used for home automation and control systems
- Operates on a mesh network topology
- Use cases: home automation, industrial automation, smart energy
- Example devices: smart thermostats, home security systems, lighting controls, industrial sensors

Bluetooth

- Provides short-range wireless communication between devices
- Low power consumption
- Allows devices to connect and communicate with each other
- Use cases: wireless audio, wearable devices, file sharing
- Example devices: wireless headphones, smartwatches, fitness trackers, wireless speakers, computer peripherals

Cellular – Global System for Mobile (GSM) communications (3G/4G)

- Provides wireless communication over cellular networks
- Offers high-speed data transfer and global coverage
- Provides voice and data services
- Use cases: mobile communication, internet browsing, video conferencing
- Example devices: smartphones, tablets, mobile hotspots, smartwatches

Infrared

- Uses infrared light to transmit data between devices
- Requires line-of-sight between devices
- Provides short-range wireless communication
- Use cases: remote controls, data transfer between devices
- Example devices: TV remote controls, cameras, printers

Ethernet

- Provides wired connection between devices
- Offers high-speed data transfer
- Requires physical connection between devices
- Use cases: internet connectivity, file sharing, media streaming
- Example devices: desktop computers, servers, network-attached storage (NAS) devices, gaming consoles

2.1.3 Understand the features, functions, and use of network standards and protocols:

- Transmission Control Protocol/ Internet Protocol (TCP/IP)
- Voice Over Internet Protocol (VOIP)
- Session Initiation Protocol (SIP)
- 7-layer Open Systems Interconnection (OSI) Model

Transmission Control Protocol/ Internet Protocol (TCP/IP)

- A suite of communication protocols used to connect devices on the internet
- Provides reliable, ordered, and error-checked delivery of packets
- Handles routing of data between networks and includes addressing schemes to identify and locate devices
- Enables end-to-end communication across the internet

Voice Over Internet Protocol (VOIP)

- Technology that enables voice communication over internet protocol (IP) networks

- Transforms analog voice signals into digital data that can be transmitted over the internet
- Allows for cost-effective and efficient communication, especially for long-distance or international calls
- Includes features such as call waiting, voicemail, and conference calling

Session Initiation Protocol (SIP)

- A signalling protocol used to initiate, maintain, and terminate real-time sessions that involve video, voice, messaging, and other communications applications and services between two or more endpoints on IP networks
- Enables users to establish and manage communications sessions such as voice and video calls, and conference calls
- Uses text-based messages to negotiate and establish sessions
- Supports features such as call forwarding, call waiting, and call hold

7-layer OSI Model

- A conceptual framework for understanding and describing network communication
- Consists of seven layers, each with its own set of protocols and functions
- The layers are: physical, data link, network, transport, session, presentation, and application
- Each layer provides services to the layer above it and uses services provided by the layer below it
- Enables communication between different types of hardware and software

2.2 Network design and implementation

2.2.1 Understand the characteristics of different network transmission media:

Wireless

- **Microwave:** used for long-distance, point-to-point communication such as satellite communication and cellular networks. Example: satellite TV transmission.
- **Radio:** used for short-range communication such as Wi-Fi and Bluetooth. Example: streaming music from a smartphone to a speaker.
- **Light:** used for high-speed, short-range communication such as infrared (IR) and visible light communication (VLC). Example: using a TV remote control to change channels.

- **Satellite:** used for long-distance, satellite-to-satellite or satellite-to-ground communication such as GPS and satellite internet. Example: using GPS to navigate in a car.

Wired

- **Copper-twisted pair and cable:** used for short to medium-range communication such as Ethernet and telephone lines. Example: connecting a computer to a router with an Ethernet cable.

- **Fibre optics:** used for high-speed, long-range communication such as internet backbone networks and cable television. Example: streaming 4K video over a fibre-optic internet connection.

- **Powerline:** uses existing electrical wiring to transmit data over short distances, typically in a home or office environment. Example: connecting a smart TV to the internet using powerline adapters.

2.2.2 Understand a variety of network metrics:

Speed

- Refers to the rate at which data can be transmitted over a network.

- Measured in bits per second (bps) or bytes per second (Bps).

- Higher speed means that data can be transferred faster over the network.

Bandwidth

- Refers to the maximum amount of data that can be transmitted over a network in a given time.

- Measured in bits per second (bps) or bytes per second (Bps).

- A higher bandwidth means that more data can be transferred over the network.

- Essentially the same as speed

Throughput

- Refers to the actual amount of data that is transferred over a network.

- Measured in bits per second (bps) or bytes per second (Bps).

- Throughput is always lower than the network's bandwidth due to various factors such as network congestion, errors, and retransmissions.

Scalability

- Refers to a network's ability to accommodate an increasing number of users or devices.
- A scalable network can handle more users or devices without experiencing a decrease in performance or functionality.

Latency

- Refers to the time delay that occurs when data is transmitted over a network.
- Measured in milliseconds (ms).
- Low latency means that data can be transmitted quickly and efficiently over the network.

Error rate

- Refers to the number of errors that occur during data transmission.
- Measured as a percentage of the total number of packets transmitted.
- A lower error rate indicates a more reliable network.

Packet loss

- Refers to the percentage of data packets that are lost during transmission.
- Packet loss can be caused by network congestion, errors, or other issues.
- A lower packet loss rate indicates a more reliable network.

Availability

- Refers to the amount of time that a network is available for use.
- Measured as a percentage of total time.
- A higher availability means that the network is more reliable and accessible.

Jitter

- Refers to the variation in latency that can occur during data transmission.
- Measured in milliseconds (ms).
- Low jitter means that data can be transmitted smoothly and without delay.

2.2.3 Understand the role of components in networks:

Switch

A switch is a network device that connects devices together on a local area network (LAN). It forwards data packets between devices based on their Media Access Control (MAC) addresses.

Switches connect clients to a network.

Bridge

A bridge is similar to a switch in that it also connects devices together on a LAN. However, bridges operate at the Data Link layer of the OSI model and use MAC addresses to filter and forward network traffic between LAN segments.

Bridges connect two or more networks.

Gateway

A gateway is a network device that connects two networks that use different protocols or technologies. It translates data between the two networks and manages their communication.

Essentially a smart bridge.

Router

A router is a device that connects two or more networks and forwards data packets between them based on their IP addresses. It acts as an intermediary between networks, enabling communication between them.

Multi-function device

A multi-function device is a combination of a router and a switch. It allows for the creation of a LAN and the connection of the LAN to the Internet.

Modem

A modem is a device that modulates and demodulates digital data for transmission over analog telephone lines or cable lines. It converts digital signals into analog signals and vice versa.

Repeater

A repeater is a device that amplifies and retransmits signals on a network. It is used to extend the range of a network by regenerating the signal and boosting its strength.

Server

A server is a computer that provides resources or services to other computers on a network. It can be used for file storage, printing, or running applications.

Network Interface Card (NIC)

A NIC is a hardware component that enables a computer to connect to a network. It allows the computer to communicate with other devices on the network.

Wireless Access Point

A wireless access point is a device that allows wireless devices to connect to a wired network. It broadcasts a wireless signal and enables devices to connect to the network using Wi-Fi.

Hubs

A hub is a network device that connects multiple devices on a LAN. It receives data packets from one device and broadcasts them to all other devices on the network, regardless of their MAC addresses. Hubs are generally less efficient than switches or bridges and are less commonly used in modern networks.

Essentially a stupid switch/bridge.

2.2.4 Be able to produce outline designs for networks to meet specified requirements that take account of location of devices.

2.2.5 Understand the characteristics and function of:

IP addressing is a fundamental aspect of computer networking, used to uniquely identify devices on a network. Here's an overview of the characteristics and functions of different types of IP addressing:

Internet Protocol version 4 (IPv4)

IPv4 is the most widely used version of IP addressing. It uses 32-bit addresses and can support up to approximately 4 billion unique addresses. IPv4 addresses are typically represented in dotted decimal notation (e.g., 192.168.1.1) and are divided into two parts: the **network ID** and the **host ID**. The network ID identifies the network, while the host ID identifies the individual device on that network.

Internet Protocol version 6 (IPv6)

IPv6 is the successor to IPv4 and uses 128-bit addresses, which provides an almost unlimited number of unique addresses. IPv6 addresses are typically represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) and are divided into three parts: **the network prefix**, **the subnet ID**, and the **interface ID**. This addressing scheme offers more efficient routing, improved security, and easier network management.

Static IP addressing

A static IP address is manually assigned to a device and remains fixed. It doesn't change unless manually modified, and it ensures that the device always has the same IP address. Static IP addressing is commonly used for servers, printers, and other network devices that require a consistent IP address for other devices to access them.

Dynamic IP addressing

A dynamic IP address is assigned to a device by a DHCP server and can change periodically. When a device connects to a network, it sends a request for an IP address to the DHCP server, which responds with an available IP address. Dynamic IP addressing is commonly used for end-user devices such as laptops, smartphones, and tablets.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol used to automatically assign IP addresses and other network settings to devices on a network. It enables network administrators to centrally manage and allocate IP addresses, making it more efficient and scalable than manually assigning IP addresses. DHCP servers can be configured to provide other network settings such as subnet masks, default gateways, and DNS server addresses.

In summary, IP addressing is a critical aspect of computer networking that enables devices to communicate with each other over a network. Different types of IP addressing and protocols, such as IPv4, IPv6, static addressing, dynamic addressing, and DHCP, offer various benefits and drawbacks, depending on the specific network requirements.

Media Access Control (MAC) Addressing

- MAC addressing is a unique 48-bit identifier assigned to network interface controllers.
- It is used in the data link layer (OSI Model) to control network access and ensure data is transmitted to the correct device.
- MAC addresses are permanent and cannot be modified by end-users.
- They are used in conjunction with protocols like ARP (gets the MAC address) to enable device communication on a network.
- MAC addresses are essential for the proper functioning of network devices and the Ethernet protocol.
- They can be used for security purposes to restrict access to a network.
- MAC addresses are used in virtualization and wireless environments.
- In short, MAC addressing is critical for networking and device communication.

2.3 Network security

2.3.1 Understand the impact of network security issues on individuals and organisations (threats and solutions, open networks).

Threats

There are numerous network security threats that can impact individuals and organisations, such as malware, phishing attacks, denial-of-service attacks, data breaches, and

unauthorised access to networks and devices.

Impact on individuals

Network security threats can lead to personal data theft, identity theft, financial losses, loss of privacy, and exposure to malicious content.

Impact on organisations

Network security threats can cause significant damage to an organisation, such as loss of confidential data, financial losses, reputational damage, legal consequences, and disruption of business operations.

Solutions

To address network security threats, individuals and organisations can implement security measures such as firewalls, antivirus software, intrusion detection and prevention systems, access control policies, encryption, and regular security audits and training.

Open networks

Open networks, such as public Wi-Fi networks, can pose a significant threat to network security. They may lack encryption and other security measures, making them vulnerable to attacks. Individuals and organisations should avoid using open networks for sensitive tasks and use a virtual private network (VPN) for added security.

Cybersecurity awareness

Raising cybersecurity awareness among individuals and employees is critical to preventing network security threats. This includes educating them on safe online practices, recognizing phishing emails, using strong passwords, and keeping software and security measures up to date.

In summary, network security threats can have severe consequences for individuals and organisations. Implementing security measures, avoiding open networks, and raising cybersecurity awareness are critical to preventing and mitigating network security threats.

2.3.2 Understand how to secure a network using both hardware and software:

Firewall

- Install a firewall to block unauthorised access to the network and prevent external attacks.
- Configure the firewall to restrict traffic to and from the network based on predefined rules.
- Use a hardware firewall for added security
    - Top-view centralised security
    - All data passes through it

    - Don’t have to configure software firewalls individually

Security settings

- Configure security settings for network devices such as routers, switches, and servers.
- Disable unnecessary services and ports to reduce the attack surface.
- Use secure protocols such as HTTPS, SSH, and SSL/TLS to protect data in transit.

Anti-malware

- Install anti-malware software on all network devices to detect and remove malware.
- Ensure that the anti-malware software is up-to-date and regularly scans the network for threats.

User controls/access/rights/profile

- Implement user controls, access rights, and profiles to restrict access to network resources.
- Create separate user accounts with different levels of access based on job roles and responsibilities.
- Regularly review and update user access rights and profiles to ensure they are appropriate and up-to-date.

Authentication types

- Use strong authentication methods such as passwords, two-factor authentication, and biometrics to verify user identities.
- Require users to create strong passwords that are difficult to guess and regularly change them.
- Use two-factor authentication to provide an additional layer of security.

Encryption techniques

- Use encryption techniques to protect sensitive data on the network.
- Use encryption protocols such as WPA2 for wireless networks and SSL/TLS for web traffic.
- Encrypt data stored on devices and backup media.

Physical controls

- Implement physical controls to prevent unauthorised access to network devices and

resources.

- Use locks, surveillance cameras, and access control systems to secure server rooms and data centres.

- Ensure that network devices are physically secure and cannot be tampered with.

Topic 3: The online environment

The internet and the world wide web are fundamental parts of our digital activity. The rise of cloud storage and cloud computing require more online activity. As more and more people work online and participate in online communities, the issues of potential and risk need to be considered.

What students need to learn

3.1 The internet and the world wide web

3.1.1 Understand what is meant by the internet and how it is structured (Internet Protocol (IP) addressing and Domain Name System (DNS)).

- The Internet is a global network of interconnected devices that communicate using standardised protocols.

- The Internet is structured using a hierarchical addressing system called Internet Protocol (IP) addressing. IP addresses uniquely identify devices on the Internet and allow for the routing of data packets between them.

- IP addresses are divided into two versions: IPv4 and IPv6.

- The Domain Name System (DNS) is a decentralised naming system that maps domain names to IP addresses, making it easier for users to access resources on the Internet.

- DNS servers store and maintain domain name records and allow users to access websites by typing in domain names instead of IP addresses.

- The DNS system is organised into a hierarchical structure that includes top-level domains (TLDs) such as .com, .org, and .edu, and subdomains that are assigned to specific organisations and websites.

- Internet Service Providers (ISPs) provide access to the Internet for individuals and organisations by connecting them to the global network through their networks and infrastructure.

3.1.2 Understand the features, functions, impact, and potential of the world wide web.

- The World Wide Web (WWW or Web) is an information system that allows users to access and share multimedia resources (e.g., text, images, videos) over the Internet.
- The Web is built on top of the Internet and uses standard protocols such as HTTP, HTML, and URL to allow users to navigate and interact with web pages and resources.
- The Web has a decentralised architecture that allows anyone to create and publish web pages and resources, making it a powerful platform for information dissemination and collaboration.
- The Web has transformed many industries and sectors, including education, commerce, entertainment, and communication, by enabling new forms of interaction, engagement, and innovation.
- The Web has also brought about new challenges and issues, including online security, privacy, and digital divide, which require ongoing attention and solutions.
- The Web has the potential to enable new technologies and applications, such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, that can further transform and improve our lives and societies.
- The Web has become an essential part of our daily lives and activities, and it is expected to continue to evolve and shape our future in significant ways.

3.1.3 Understand the difference between static and dynamic web page content, and the need to use the different types.

3.1.4 Understand the role of client-side scripting.

3.1.5 Understand the role of server-side scripting.

Static Web Page Content

- Content that remains the same regardless of user input or other external factors.
- Typically written in HTML, CSS, and JavaScript, and stored as files on a web server.
- Easy to create and maintain, and can be served quickly and efficiently to users.
- Suitable for websites that have little or no need for user interaction or personalised content.

Dynamic Web Page Content

- Content that changes based on user input or other external factors, such as database updates, API calls, or server-side scripting.
- Can be created using various technologies, such as PHP, ASP, Python, or JavaScript.
- Allows for user interaction, personalization, and real-time updates.
- Suitable for websites that require user input, custom content, or real-time data updates.

The Need for Static and Dynamic Web Page Content

- Static web pages are best for simple websites that don't require much user interaction or personalised content.
- Dynamic web pages are better suited for websites that require real-time updates, user input, or personalised content.
- A combination of static and dynamic web pages can provide the best user experience and functionality for a website.
- The choice of static or dynamic web page content depends on the website's purpose, audience, and functionality requirements.

Server-side Scripting

- Server-side scripting is executed on the server before the web page is sent to the client's browser.
- Server-side scripting is used to generate dynamic content, process user input, and interact with databases and other backend systems.
- Server-side scripting languages include PHP, Python, Ruby, and others.
- Server-side scripting is more secure and efficient but requires more resources and expertise.

Client-side Scripting

- Client-side scripting is executed on the client's browser after the web page is loaded.
- Client-side scripting is used to add interactivity, animations, and other visual effects to the web page, without requiring a round trip to the server.
- Client-side scripting languages include JavaScript, HTML5, and CSS3.
- Client-side scripting is more user-friendly and responsive but can be less secure and more resource-intensive.

Use of Server-side and Client-side Scripting

- The use of server-side and client-side scripting depends on the specific requirements and goals of the website and the resources and expertise available to the developers.

- A well-designed web application usually employs a combination of server-side and client-side scripting to achieve the desired functionality, performance, and user experience.

- Server-side scripting is more suitable for complex data processing and security-sensitive tasks, while client-side scripting is more suitable for user interface design and real-time updates.

- The combination of server-side and client-side scripting can improve website performance, reduce server load, and enhance user experience.

3.2 Operating online

3.2.1 Understand the impact and potential of working in online environments for individuals and organisations.

Impact

- Increased flexibility and accessibility for individuals and organisations, enabling remote work and collaboration from anywhere in the world.

- Improved efficiency and productivity through streamlined workflows, real-time communication, and access to vast amounts of information and resources.

- Enhanced creativity and innovation through new technologies, tools, and platforms that facilitate collaboration and experimentation.

- Increased competition and disruption in traditional industries, as digital technologies and online platforms enable new business models and disrupt established players.

- Greater risk of cyber threats, data breaches, and privacy violations, as online environments expose individuals and organisations to new forms of security risks.

Potential

- Expanded reach and audience for individuals and organisations, as online environments enable global connectivity and access to diverse communities and markets.

- New opportunities for entrepreneurship and innovation, as online platforms and technologies enable low-cost and scalable business models and new forms of value creation.

- Improved access to education and knowledge, as online learning platforms and resources democratise access to information and skills.

- Increased social and political engagement, as online platforms and communities enable new forms of activism, expression, and participation.

- Greater potential for sustainability and social impact, as online platforms and technologies enable new forms of collaboration, resource-sharing, and collective action.

3.2.2 Understand the security risks to personal data stored online and methods of protection.

Security Risks

- Data breaches: Unauthorised access to personal data stored online through hacking, phishing, or malware attacks.

- Identity theft: Personal data stored online can be used to steal identities and perpetrate fraud.

- Privacy violations: Personal data can be used to track individuals' online activity, behaviour, and preferences without their consent.

- Malware infections: Downloading or accessing malicious software can infect personal devices and compromise stored data.

- Social engineering: Online attackers can manipulate individuals into divulging personal information or credentials through deception and manipulation.

Protection Methods

- Strong passwords and authentication: Using unique, complex passwords and two-factor authentication can prevent unauthorised access to personal accounts.

- Encryption: Encrypting personal data stored online can prevent unauthorised access and ensure privacy.

- Regular software updates and patches: Keeping software and operating systems up to date can prevent vulnerabilities and security exploits.

- Anti-virus and anti-malware software: Installing and regularly updating anti-virus and anti-malware software can prevent infections and protect personal data.

- Awareness and education: Educating individuals on the risks and best practices for online security can prevent social engineering and increase vigilance.

3.2.3 Understand what a digital footprint (active, passive) is and the positive and negative aspects of these.

Digital Footprint

A digital footprint is the digital trail that individuals leave behind as they interact with various online platforms and services. It can include any information that people share online, including social media posts, comments, photos, videos, and search history.

Active Digital Footprint

An active digital footprint is the information that individuals intentionally share online. This can include social media posts, comments, and other content that people create and publish on the internet.

Positive Aspects

- Can help individuals build their personal brand and establish themselves as thought leaders or experts in their field.
- Can be used to showcase skills and accomplishments to potential employers or clients.
- Can be used to connect with like-minded individuals or build a network of professional contacts.

Negative Aspects

- Can lead to reputational damage if the content shared is offensive or inappropriate.
- Can be used by hackers or cybercriminals to gain access to personal information or commit identity theft.
- Can be used by potential employers or clients to discriminate against individuals based on their personal beliefs or opinions.

Passive Digital Footprint

A passive digital footprint is the information that individuals unintentionally leave behind as they browse the internet. This can include search history, cookies, and other data that is collected by websites and online services.

Positive Aspects

- Can be used to personalise online experiences and provide users with more relevant content.
- Can help companies improve their products and services by analysing user behaviour and preferences.
- Can be used to monitor and prevent fraudulent activity online.

Negative Aspects

- Can be used to track individuals and collect personal data without their consent.

Notes by @uzayermasud

- Can be used to create targeted advertising campaigns that invade users' privacy.
- Can be used by governments or other organisations to monitor and censor online activity.

3.3 Online communities

3.3.1 Understand the concept of an online community and that online communities exist for social and professional purposes.

Online Community

An online community is a group of individuals who interact and share information and resources through online platforms such as social media, forums, or messaging apps. Online communities can be formed around a common interest, goal, or identity.

Social Online Communities

Social online communities are formed around common interests, hobbies, or lifestyle choices. They serve as a way for individuals to connect with others who share similar interests, regardless of physical location.

Examples:

- Reddit: a social news and discussion platform where users can share and discuss content on a wide range of topics.
- Instagram: a photo and video sharing app where users can follow and connect with other users based on shared interests or hobbies.
- TikTok: a video sharing app where users can create and share short-form videos around various topics, interests, and challenges.

Professional Online Communities

Professional online communities are formed around a specific industry, profession, or skill set. They serve as a way for professionals to connect with others in their field, share knowledge and resources, and collaborate on projects.

Examples:

- LinkedIn: a professional social networking site where users can connect with other professionals, search for job opportunities, and share industry news and insights.
- GitHub: a platform for software developers to collaborate on code, share knowledge, and contribute to open-source projects.
- Stack Overflow: an online community for programmers to ask and answer technical questions, share knowledge and resources, and build their professional reputation.

Online communities serve as a way for individuals to connect and collaborate with others

who share common interests or professional goals, regardless of physical location or other barriers.

3.3.2 Understand the impact of online communities on individuals and organisations.

Impact on Individuals

- Provides a sense of belonging and connection with like-minded individuals.
- Facilitates the sharing of knowledge, resources, and experiences with others.
- Offers opportunities for personal and professional development through collaboration and networking.
- Can help individuals build their personal brand and establish themselves as thought leaders in their field.
- Can also lead to negative impacts such as online harassment, bullying, and exposure to harmful content or ideas.

Impact on Organisations

- Provides a way for organisations to engage with their customers or users and gather feedback and insights.
- Can help organisations build brand loyalty and community around their products or services.
- Offers a platform for knowledge sharing and collaboration among employees or team members.
- Can lead to increased innovation and problem-solving through collaboration and idea sharing.
- Can also lead to negative impacts such as reputational damage due to negative online reviews or social media backlash.

Online communities have the potential to bring about significant positive impacts for individuals and organisations, such as increased collaboration, knowledge sharing, and innovation. However, they can also have negative impacts, such as exposure to harmful content, reputational damage, and online harassment, which must be carefully managed and addressed.

3.3.3 Understand the monetisation opportunities provided by online communities:

Use of Customer Data with Targeted Advertising

Online communities can collect data on users' interests, demographics, and behaviours, and

use this information to deliver targeted advertising to users. This can generate revenue for the community platform and for advertisers.

Pay-Per-Click Advertising

Community platforms can offer pay-per-click advertising opportunities to advertisers, where they pay each time a user clicks on their ad. This can generate revenue for the community platform and for the advertiser.

Selling of Customer Data

Online communities can sell user data to third-party companies for market research or other purposes. This can generate revenue for the community platform, but **may raise privacy concerns** among users.

Paid Subscriptions (Paywalls)

Community platforms can offer paid subscriptions or paywalls, where users must pay to access premium content or features. This can generate revenue for the community platform and offer a way for users to support the community.

Sponsored Content

Community platforms can offer sponsored content opportunities to advertisers, where they pay to have their content featured or promoted within the community. This can generate revenue for the community platform and for the advertiser.

Overall, monetization opportunities in online communities can provide a way for the community platform to generate revenue and sustain itself, while also offering opportunities for advertisers to reach their target audience in a targeted and engaging way. However, it's important to consider the privacy and ethical implications of using customer data and to ensure that any monetization strategies align with the community's values and goals.

3.4 The cloud

3.4.1 Understand the concept, use and impact of cloud storage.

3.4.2 Understand the concept, use and impact of cloud computing.

Cloud Storage

Cloud storage is a service that allows users to store, access, and manage data over the internet, rather than on local storage devices. This data can be accessed from any device with an internet connection.

Uses

- Storing and sharing files and documents with others
- Collaborating on projects and documents with others in real-time
- Storing and accessing media files such as photos, videos, and music

- Backing up data to prevent loss in the event of hardware failure or disasters
- Hosting websites and web applications

Cloud Computing

Cloud computing is a service that provides on-demand access to computing resources, such as servers, storage, and applications, over the internet. Users can access these resources without needing to invest in and maintain their own infrastructure.

Uses:

- Hosting websites and web applications
- Running software applications without needing to install them locally
- Analysing large datasets for research or business purposes
- Running virtual machines for development or testing purposes
- Scaling computing resources up or down based on demand

Impact of Cloud Storage and Cloud Computing

- Provides easy and convenient access to computing resources and data from anywhere with an internet connection
- Offers cost savings by reducing the need for users to invest in and maintain their own infrastructure
- Facilitates collaboration and teamwork by allowing multiple users to access and work on the same files or applications simultaneously
- Enables scalability, allowing organisations to quickly and easily adjust computing resources based on demand
- Raises security and privacy concerns related to data storage and access over the internet.

Cloud storage and cloud computing have revolutionised the way individuals and organisations store, access, and manage data and computing resources. They offer convenience, cost savings, and scalability, but also raise important security and privacy concerns that must be carefully considered and addressed.

Topic 4: IT systems

IT systems are pervasive in organisations. They are used for stock control, booking, asset management, and logistics. These systems operate effectively because they are designed

and planned. An understanding of conventional notation will enable students to design systems consisting of both hardware and software components.

What students need to learn

4.1 Systems design

4.1.1 Understand the concept of an IT system:

Hardware

The physical components of an IT system, such as computers, servers, storage devices, and networking equipment. Hardware provides the underlying infrastructure for an IT system to function.

Software

The programs and applications that run on IT system hardware, such as operating systems, productivity software, database management systems, and security software. Software is essential for performing various tasks and functions within an IT system.

Processes

The procedures and workflows that define how an IT system operates and how tasks are performed within the system. Processes can be automated or manual and can involve multiple components of the IT system.

People

The individuals who operate and maintain the IT system, including IT professionals, end-users, and stakeholders. People are essential for ensuring the IT system is functioning effectively and efficiently.

4.1.2 Understand how to decompose a system into smaller subsystems and components.

Look at specification point 2.2.3 and question papers

4.1.3 Be able to design IT systems, from individual components and subsystems, to meet specified requirements. (Symbols are given in *Appendix 7*.)

Look at specification point 2.2.3 and question papers

4.1.4 Understand the concept of 'fitness for purpose' when evaluating systems.

- Set of requirements
- Measurable criteria
- Agreement with customer/client

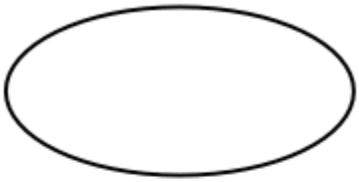
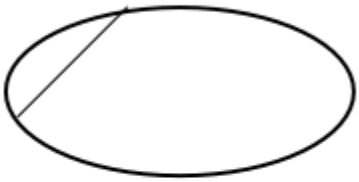
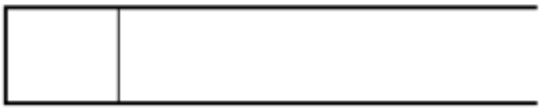
4.2 Dataflow

4.2.1 Understand the concept of and the need for data flow diagrams.

- Creates an overview of the system
- Helps visualise the process/dataflow
- Avoids excessive detail at an early stage
- Can be drawn at different levels of complexity
- Allows top-down expansion
- Easy to explain to non-technical audiences
- Shows the system boundaries
- Shows flow to external entities

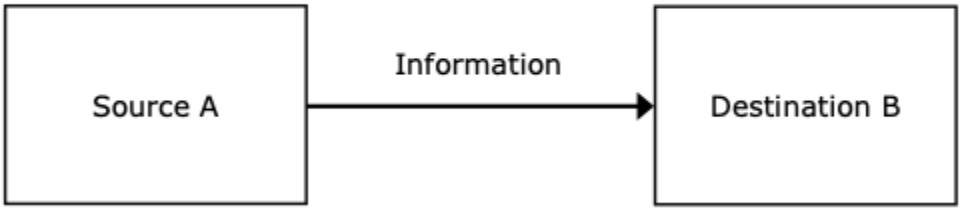
4.2.2 Be able to interpret and create data flow diagrams for a given scenario. (Symbols are given in *Appendix 7*.)

Data Flow Symbols

Purpose	Symbol
Data source or destination (inputs and outputs)	
Duplication data source or destination	
Process	
Data store	

Information Flow

Students should be able to use and create appropriately labelled diagrams to express meaning.



Data and Information Flow Diagrams

4.3 Flowcharts

4.3.1 Understand the concept of and the need for flowcharts.

Flowcharts are visual representations of a process or system that use symbols and diagrams to illustrate the steps involved in completing a task or achieving a goal.

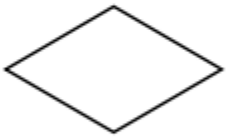
Need for Flowcharts

- Provide a clear and concise overview of a process or system
- Identify potential problems or inefficiencies in a process
- Standardise processes and procedures for consistent results
- Facilitate communication and collaboration among team members
- Aid in training and onboarding new employees
- Serve as a tool for analysis and improvement of a process or system

4.3.2 Be able to interpret and create flowcharts for a given scenario. (Symbols are given in *Appendix 7*.)

IGCSE Computer Science

Flowcharts

Purpose	Symbol
Input/Output	
Process	
Subprocess	
Decision	
Terminator	
Labels	Yes No
Flow	

4.4 Systems

4.4.1 Understand the advantages and disadvantages of IT systems for individuals and organisations.

Advantages

- Improved efficiency and productivity through automation of tasks
- Greater access to information and communication, enabling collaboration and

knowledge sharing

- Enhanced decision-making capabilities through data analysis and visualisation
- Increased convenience and flexibility through remote work and mobile devices
- Potential cost savings through reduced need for physical infrastructure and streamlined processes

Disadvantages

- Dependence on technology, making individuals and organisations vulnerable to system failures, cyber attacks, and data breaches
- Potential loss of privacy and security of personal and sensitive data
- Risk of job displacement due to automation and outsourcing of tasks
- Initial and ongoing costs associated with purchasing, implementing, and maintaining IT systems
- Risk of technology obsolescence, requiring regular updates and upgrades to remain competitive

4.4.2 Understand how a range of contemporary digital devices, peripheral devices, storage devices and memory are used in IT systems to meet the needs of individuals and organisations.

See specification point 2.2.3 and question papers

Topic 5: Data and databases

Our digital world runs on data. Whether it is personal data or institutional data, it must be organised in such a way that it can be retrieved, manipulated, and understood to have value. Databases are one way in which data is organised, retrieved and manipulated.

What students need to learn

5.1 Data and information

5.1.1 Understand the difference between data and information.

Data

Refers to raw, unprocessed, and unorganised facts or figures that are collected and stored by various sources.

Information

Refers to data that has been processed, organised, and analysed in a way that makes it meaningful, useful, and actionable.

Key differences

- Data is raw and unprocessed, while information is processed and organised.
- Data is not useful on its own, while information provides insights and knowledge.
- Data is the input for generating information, while information is the output of data processing.
- Data is usually represented as numbers or text, while information can be represented in various formats, such as graphs, charts, reports, and dashboards.

5.1.2 Understand sources of and the difference between structured and unstructured data.

Sources of data

Data can come from a variety of sources, such as:

- Business transactions, such as sales or inventory records
- Social media interactions, such as tweets or comments
- Web logs, such as website visitor data or clickstream data
- Sensors, such as temperature or location data
- Audio and video recordings, such as surveillance footage or customer service calls

Structured data

Refers to data that is organised and formatted in a specific way that makes it easy to search, analyse, and process. Structured data is typically stored in databases or spreadsheets and can be easily queried and analysed using software tools. Examples of structured data include:

- Customer names and addresses
- Sales transactions
- Financial data
- Inventory records

Unstructured data

Refers to data that is not organised or formatted in a specific way and is more difficult to search, analyse, and process. Unstructured data is typically stored in text-based files, such as emails, social media posts, or documents, and may contain a mix of text, images, and other multimedia elements. Examples of unstructured data include:

- Emails and chat logs
- Social media posts and comments
- Images and videos
- Audio recordings

Key differences

- Structured data is organised and formatted, while unstructured data is not.
- Structured data is easier to analyse and process, while unstructured data requires more advanced tools and techniques.
- Structured data is typically generated by internal systems and processes, while unstructured data is often generated by external sources.
- Structured data is more easily stored and managed, while unstructured data requires more storage capacity and management resources.

5.1.3 Understand the value to organisations of extracting meaningful information from data.

Extracting meaningful information from data helps organisations

- make better decisions
- improve efficiency
- enhance customer experience
- gain competitive advantage
- increase revenue
- mitigate risks
- foster collaboration.

5.2 Structured data

5.2.1 Understand why databases are used to structure data

Data organisation

Databases provide a structured way to store and organise data, making it easier to find and retrieve information.

Data integration

Databases can integrate data from multiple sources and applications, providing a unified view of data that can be accessed by multiple users.

Data security

Databases offer built-in security features to protect sensitive data from unauthorised access and data breaches.

Data consistency

Databases can enforce data consistency and integrity rules, ensuring that data is accurate, complete, and up-to-date.

Data scalability

Databases can handle large volumes of data and can scale to meet the needs of growing organisations.

Data accessibility

Databases can provide fast and efficient access to data, even for complex queries or large datasets.

5.2.2 Understand the structure of a relational database

Tables

A relational database consists of one or more tables, which are used to organise and store data. Each table represents a collection of related data that has a unique name.

Fields

Each table contains fields, which are used to store individual pieces of data. A field represents a single category of data, such as a name, date, or amount.

Records

A record is a collection of related fields that describe a single instance of the data being stored. Each record represents a unique entry in the database.

Primary keys

A primary key is a unique identifier for each record in a table. It is used to ensure that each record can be uniquely identified and to enforce data integrity constraints.

Foreign keys

A foreign key is a field in one table that refers to the primary key of another table. It is used to create relationships between tables and to enforce referential integrity constraints.

Composite keys

A composite key is a combination of two or more fields that together uniquely identify a record in a table. It is used when a single field cannot uniquely identify a record.

Relational Databases and Key Fields

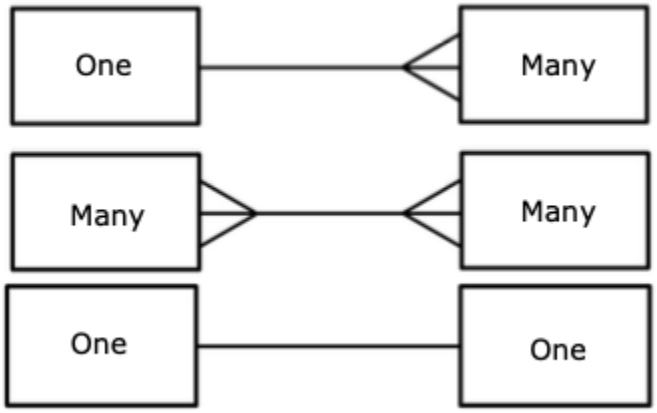
The structure of a relational database is designed to ensure that data is organised, stored, and accessed efficiently and accurately. By using tables, fields, records, primary keys, foreign keys, and composite keys, relational databases can represent complex data relationships and enforce data integrity constraints, making them an effective tool for managing and analysing large volumes of data.

5.2.3 Understand the concept of entities and the relationships between them:

Entities

An entity is a distinct object or concept that is represented in a database. Each entity has attributes that describe the characteristics of the entity, such as name, address, or age.

Entity relationship symbols



One-to-one relationship

A one-to-one relationship is a type of relationship between two entities where each entity in the relationship can be associated with only one instance of the other entity.

One-to-many relationship

A one-to-many relationship is a type of relationship between two entities where one entity can be associated with many instances of the other entity, but the other entity can be associated with only one instance of the first entity.

Many-to-many relationship

A many-to-many relationship is a type of relationship between two entities where each instance of one entity can be associated with many instances of the other entity, and vice versa.

5.2.4 Be able to interpret and create entity relationship diagrams for a given scenario. (Symbols are given in *Appendix 7*.)

See above and question papers

5.3 Structured query language (SQL)

5.3.1 Understand how and why SQL is used to manipulate data and data structures.

- used to manage and manipulate data in relational databases
- create and modify the structure of a database, including tables, fields, and relationships between tables.
- insert, update, and delete data in a database.
- query data in a database to retrieve specific information based on certain criteria.

- create views, which are virtual tables that are based on the result of a SQL statement.
- create and manage user accounts and permissions for accessing a database.

5.3.2 Know how to select and use appropriate SQL commands, features and functions to manipulate data:

Sure, here's a brief explanation of how to select and use appropriate SQL commands, features, and functions to manipulate data.

Perform queries and subqueries

- Use the SELECT statement to retrieve data from one or more tables.
- Use the WHERE clause to filter data based on specific criteria.
- Use the GROUP BY clause to group data based on specific columns.
- Use the HAVING clause to filter groups based on specific criteria.
- Use the ORDER BY clause to sort data based on specific columns.
- Use subqueries to retrieve data from nested queries.

Example:

```
SELECT column1, column2
FROM table1
WHERE column1 = 'value'
GROUP BY column2
HAVING COUNT(*) > 1
ORDER BY column2 ASC;
```

Create tables using appropriate data types

- Use the CREATE TABLE statement to create a new table.
- Use the appropriate data types for each column, such as VARCHAR, INT, DATE, etc.

Example:

```
CREATE TABLE table1 (
```

```
    column1 VARCHAR(50),
    column2 INT,
    column3 DATE
);
```

Populate tables/insert, amend, delete

- Use the INSERT INTO statement to add new records to a table.
- Use the UPDATE statement to modify existing records in a table.
- Use the DELETE statement to remove records from a table.

Example:

```
INSERT INTO table1 (column1, column2, column3)
VALUES ('value1', 123, '2023-05-06');

UPDATE table1
SET column1 = 'new_value'
WHERE column2 = 123;

DELETE FROM table1
WHERE column2 = 123;
```

Link tables(UNION, JOIN)

- Use the UNION operator to combine the results of two or more SELECT statements into a single result set.
- Use the JOIN clause to combine data from two or more tables based on a common column.

Example:

```
SELECT column1, column2
FROM table1
UNION
SELECT column1, column2
FROM table2;
```

Notes by @uzayermasud

```
SELECT table1.column1, table2.column2
FROM table1
INNER JOIN table2
ON table1.id = table2.table1_id;
```

5. Use wildcards(% and _):

- Use the % wildcard to match any sequence of characters.
- Use the _ wildcard to match any single character.

Example:

```
SELECT column1
FROM table1
WHERE column1 LIKE 'value%';

SELECT column1
FROM table1
WHERE column1 LIKE 'v_lue';
```

Group, order, count

- Use the GROUP BY clause to group data based on specific columns.
- Use the ORDER BY clause to sort data based on specific columns.
- Use the COUNT function to count the number of records in a table or group.

Example:

```
SELECT column1, COUNT(*) AS count
FROM table1
GROUP BY column1
ORDER BY count DESC;
```

Topic 6: Wider issues

The pervasive use of technology has an impact, not just for individuals, but also for the environment and society as a whole. The ability to make judgements about technology is underpinned by an understanding of the moral and ethical issues and the legal frameworks that are part of our lives.

What students need to learn

6.1 Environmental

6.1.1 Understand the environmental impact of construction, use and disposal of information technology equipment.

Construction

- Extraction of raw materials required for the manufacturing process can lead to land and water pollution, deforestation, and soil erosion.
- Energy-intensive manufacturing processes require significant amounts of electricity and generate greenhouse gas emissions.
- Manufacturing of certain components of IT equipment requires the use of hazardous chemicals, which can have negative impacts on both the environment and human health.

Use

- IT equipment consumes significant amounts of energy during its use, which can contribute to greenhouse gas emissions and global warming.
- Overuse and inefficient use of IT equipment can lead to unnecessary energy consumption, which can increase energy costs and exacerbate the environmental impact.

Disposal

- Improper disposal of IT equipment can result in e-waste, which can contaminate soil and water sources and pose a threat to human health.
- E-waste contains hazardous chemicals that can release toxic substances into the environment when not disposed of properly.
- Landfills and incineration of e-waste can result in the emission of toxic gases and contribute to air pollution and climate change.

6.1.2 Understand the positive impact that information technology makes on environmental monitoring (including smart houses and smart cities) and efficient use of resources.

Environmental Monitoring

- IT solutions can help monitor air quality, water quality, and weather conditions, providing valuable data for environmental research and decision-making.

- Smart sensors and remote monitoring technologies can detect and track changes in the environment, allowing for more efficient and timely responses to environmental issues.

- Advanced analytics and machine learning algorithms can analyse data collected from environmental sensors and provide insights for environmental management and policy-making.

Efficient Use of Resources

- IT solutions can help optimise resource usage, such as energy and water, through real-time monitoring and control.

- Smart home technologies can adjust heating, cooling, and lighting based on occupancy and weather conditions, reducing energy waste and saving money on utility bills.

- Smart city solutions can optimise traffic flow and public transportation systems, reducing congestion and carbon emissions.

- Cloud computing and virtualization technologies can reduce the energy consumption of data centres and IT infrastructure, leading to significant energy savings.

6.2 Legal, moral and ethical

6.2.1 Understand the legal issues associated with the use of information technology systems:

Data Protection

- Organisations must comply with data protection laws that regulate the collection, storage, and use of personal data.

- Personal data must be processed lawfully, fairly, and transparently, with appropriate security measures in place to protect against unauthorised access, loss, or theft.

- Individuals have the right to access their personal data, request that it be corrected or deleted, and object to its use for certain purposes.

Copyright

- Copyright laws protect the rights of creators of original works, including software, music, videos, and written content.

- The use or distribution of copyrighted material without permission or proper attribution is illegal and can result in legal action.

- Fair use exemptions allow for limited use of copyrighted material for certain purposes, such as criticism, commentary, or education.

Computer Misuse

- Computer misuse laws prohibit unauthorised access, modification, or damage to computer systems, networks, or data.

- Hacking, malware, and phishing attacks are examples of computer misuse that can result in criminal charges and penalties.

- Penetration testing and ethical hacking are legal ways to test the security of computer systems with permission and under specific conditions.

Intellectual Property

- Intellectual property laws protect the rights of creators of new inventions, designs, or processes, including patents, trademarks, and trade secrets.

- Organisations must respect the intellectual property rights of others and obtain appropriate licences or permissions to use patented technology or trademarks.

- Trade secret theft or misappropriation can result in legal action and damages.

6.2.2 Understand the moral and ethical issues associated with the use of information technology systems:

Privacy

- IT systems can collect and store personal data, raising concerns about privacy and the potential misuse of personal information.

- Organisations must ensure that personal data is collected and used in a transparent, lawful, and ethical manner.

- Individuals have the right to control their personal data and be informed about how it is used, shared, and protected.

Inclusion

- IT systems should be designed to be accessible to everyone, regardless of their race, gender, age, ability, or socioeconomic status.

- Organisations must ensure that their IT systems do not discriminate against any group or individual and promote equal opportunities for all.

- Inclusive design can improve the user experience and increase the adoption and effectiveness of IT systems.

Civil Liberties

- The use of IT systems can raise concerns about civil liberties, such as freedom of speech, assembly, and association.

- Organisations must ensure that their IT systems do not infringe on civil liberties and promote democratic values and principles.

- Government surveillance and censorship of online content are examples of civil

liberties issues related to the use of IT systems.

Access

- IT systems should be accessible to everyone, regardless of their location, infrastructure, or financial resources.
- Organisations must ensure that their IT systems are available to all users and do not exclude any group or individual.
- Digital divide, net neutrality, and access to education and healthcare are examples of access issues related to the use of IT systems.

Accessibility

- IT systems should be designed to be accessible to people with disabilities, such as visual, hearing, or mobility impairments.
- Organisations must ensure that their IT systems are compliant with accessibility standards and guidelines, such as the Web Content Accessibility Guidelines (WCAG).
- Assistive technologies, such as screen readers and voice recognition software, can improve accessibility and usability for people with disabilities.

Expression

- The use of IT systems can facilitate the expression of diverse views and opinions, promoting freedom of expression and democracy.
- Organisations must ensure that their IT systems do not suppress or censor legitimate expressions of opinion and promote pluralism and tolerance.
- Hate speech, cyberbullying, and online harassment are examples of expression issues related to the use of IT systems.

Association

- The use of IT systems can facilitate the formation of social groups and communities, promoting social cohesion and mutual support.
- Organisations must ensure that their IT systems do not exclude or discriminate against any group or individual and promote inclusivity and diversity.
- Online radicalization, hate groups, and online fraud are examples of association issues related to the use of IT systems.

6.3 Society

6.3.1 Understand the impact of ubiquitous wireless access:

Smart Cities

- Ubiquitous wireless access enables the creation of smart cities, where IT systems are

used to manage urban infrastructure and services.

- Smart cities can improve the efficiency and sustainability of energy, transportation, and waste management systems.

- Smart city applications, such as traffic management, smart grids, and intelligent building systems, rely on ubiquitous wireless access to collect and analyse data in real-time.

Location Awareness

- Ubiquitous wireless access enables location awareness, where IT systems can track and analyse the location of people and objects in real-time.

- Location awareness can improve the efficiency and safety of transportation systems, emergency response, and supply chain management.

- Location-based applications, such as GPS navigation, location-based advertising, and geofencing, rely on ubiquitous wireless access to provide accurate and reliable location data.